REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims **1-37** are pending in the application.

Claims **1-37** have been rejected.

Claim **1** has been amended in this submission. Applicants respectfully assert that the amendments to the claims add no new matter.

CLAIM REJECTIONS

35 U.S.C. § 102 Rejections

In the final Office action, the Examiner rejected claims 1-37 under 35 U.S.C. § 102(b), as being anticipated by Richmond et al. (U.S. Pat. Pub. No. 2003/0154380) ("Richmond"). Applicants respectfully traverse this rejection at least in view of the remarks that follow.

Richmond is directed to controlling usage of network resources but is unrelated to protecting, managing or controlling transfer of information between a computer and an external device connected to the computer.

As taught by Richmond, an entry point device such as a switch or hub controls usage of network resources by a user.

A user's <u>usage of network resources is controlled</u>, after the user has been authenticated, without using any network resources beyond the user's entry point to the network. <u>Packet rules may be provisioned to the user's entry point to the network</u>, and the packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used.

[...] <u>Usage of network resources of a communications network by a user beyond a network device of the communications network that serves as the user's entry point to the communications network is controlled</u>. The port module of the network device is configured with one or more packet rules corresponding to an identity of the user. A packet is received from a device used by the user at the port module, and, <u>before using any of the network resources beyond the network device, the one or more packet rules are applied to the received packet</u>. (Richmond, Abstract, emphasis added).

In contrast, the invention as claimed is directed to controlling a transfer of data between a computer and an external device connected to a port of the computer.

<u>Security agent 230 may be activated when a physical communication port is requested</u>. The security agent 230 may pull the <u>transportation to and from the physical communication port, processes the information and may reach a decision regarding the legality of the requested connection and/or data transfer</u>. (Application as filed, para. [0041], emphasis added).

Accordingly, the invention as claimed and the Richmond reference are directed to different fields and solve different problems. In fact, controlling a transfer of information between a computer and an external device connected to the computer would serve no purpose to Richmond which is directed to controlling usage of network resources but is unrelated to controlling the transfer of data between a computer and an external device connected to a port of the computer.

To find the element of "A method for protecting the transfer of data between a computer and an external device" the Examiner pointed to authentication and authorization in paragraph [0255] of Richmond.

However, paragraph [0255] of Richmond discloses:

By leveraging the process of authenticating and authorizing users, which can be implemented using any number of known or later developed technologies, for example, RADIUS, 802.1X, NOS

> login, Smart cards, Kerberos and biometrics, the identity of a user
> may be determined, and network usage parameters may be
> dynamically provisioned to the user's entry point to the network,
> whether wired, or wireless or a combination thereof. This
> leveraging allows the authentication process, which historically
> has provided drive, file, and system level access, to be extended to
> the edge of the network, which may provide a significant increase
> in the security, resiliency, and scalability of the network.

Clearly, although disclosing RADIUS, 802.1X, NOS login, Smart cards, Kerberos and biometrics used in authenticating and authorizing users at an entry point to the network, paragraph [0255] of Richmond is unrelated to protecting the transfer of data between a computer and an external device.

Applicants submit that authentication and/or authorization of users at an entry point to a network is unrelated, nor amounts to, protecting the transfer of data between a computer and an external device.

In order to further clarify the scope of the invention, Applicants have amended independent claim 1 to recite "A method for controlling the transfer of data between a computer and an external device connected to a port of the computer" (emphasis added). As discussed above, Richmond is directed to controlling usage of network resources but is unrelated to controlling transfer of data between a computer and an external device connected to a port of the computer.

To find the element of "receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device" the Examiner pointed to item 1502 in Fig. 15 of Richmond.

However, packets 1502 in Fig. 15 of Richmond are received from a user at a network entry point and are not a data communicated between a computer and an external device connected to the computer.

Moreover, packets 1502 are received from the user's computer by a network node. In contrast, claim 1 recites receiving a data portion from an external device by the user's computer.

To find the element of "analyzing, by said module, the data portion according to a protocol associated with the physical communication port" the Examiner pointed to the

authentication logic in paragraphs [0047]-[0048] of Richmond. However, an authentication logic to authenticate an identity of a user and configuring a port module in response to an authentication is unrelated to analyzing data according to a protocol associated with a physical communication port. Neither in paragraphs [0047]-[0048] nor elsewhere does Richmond teach, or even remotely suggest analyzing data according to a protocol associated with a physical communication port.

In fact, directed to authenticating a user, analyzing data according to a protocol associated with a specific physical communication port would serve no purpose to Richmond since the physical ports used on the user's computer and/or the network node are irrelevant to an authentication of the user.

To find the element of "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if no decision may be reached on whether to allow said data communication session, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd'" the Examiner pointed to paragraph [0048] and item 308 in Fig. 3 of Richmond.

However, storing relationship hierarchy as shown by 308 in Fig. 3 of Richmond is unrelated to storing a portion of a data communication. Richmond does not teach storing a portion of data communicated between a source and destination. Rather, Richmond teaches storing information related to rules, roles of parties etc.

> The relationship hierarchy 200 may include one or more roles 202-206, one or more service abstractions 208-214 and one or more packet rules 220-231. (Richmond, para. [0099], emphasis added).

Clearly, Richmond does not teach storing a portion of data communicated between a computer and an external device or, storing a portion of any data communicated. Rather, rules, service abstractions and other information related to communicated data are stored. Applicants note that storing information related to the data communicated (such as rules or roles) is not to be confused with storing a portion of the data communicated.

To find the element of "if said data communication session is to be allowed transferring the data portion with data stored in the associated buffer, if any exist, toward or from the physical communication port, and if said data communication session is not to be allowed, then modifying data transportation related to said data communication session" the Examiner pointed to paragraph [0046] of Richmond.

However, neither in paragraph [0046] no elsewhere does Richmond teach buffering data communicated between a computer and an external device (or buffering any other communicated data for that matter) until a decision on whether or not the session is allowed to proceed and, if so, communicate buffered data to its destination.

Richmond is directed to authenticating a user and, if the user is authenticated, data to/from the user is allowed to be communicated, otherwise, a session may be blocked. Authenticating a user is performed at the beginning of the session, before actual data is communicated. For example, as shown by 1316 in Fig 13A of Richmond.

Accordingly, buffering actual data communicated from/to a user would serve no purpose to Richmond since prior to a communication of actual data authentication is performed. If authentication of the user fails then no actual data is communicated, and communication of actual data is only performed upon successful authentication of the user, in which case there's no need for buffering data communicated to/from the user.

In light of the above discussion, independent claim 1 as amended is allowable over Richmond. The discussion above is relevant to independent claims 21 and 34 which recite similar elements and are therefore allowable over Richmond.

Each of dependent claims 2-19, 22-33 and 35-37 depends, directly or indirectly, from one of independent claims 1, 21 and 34 and includes all the features of the claim from which it depends as well as additional distinguishing features, and is therefore allowable. Accordingly, claims 2-19, 22-33 and 35-37 are allowable over Richmond.

However, some of dependent claims 2-19, 22-33 and 35-37 merit further discussion.

Regarding claims 3-5, Richmond does not teach at least the elements of "modifying the type of the transportation" (claim 3), "modifying the status of a requested file" (claim 4) or "...the step of modifying the data transportation further

comprises correcting the data" (claim 5). Richmond merely teaches rules applicable to network packets that may cause a packet to be dropped but not stored, type-modified, status-modified, or corrected.

Regarding claims 6 and 7, Richmond does not teach a physical communication port selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared. In paragraph [0006], Richmond teaches a switching device (switch, hub, router, bridge) that is part of a network and has a plurality of physical ports. No reference is made to a physical communication port that is selected from the group recited in claim 6. Likewise, directed to network ports, Richmond does not teach a physical communication port that is a USB port as recited by claim 7.

Regarding claims 9 and 10, Richmond does not teach a processing of a data portion comprising "...determining whether additional processing based on a higher level protocol is required" and "processing part of the data portion that is relevant to the higher level protocol". Furthermore, Richmond does not teach a processing that is relevant to a higher level protocol associated with the device. Processing as taught by Richmond is related to a packet, a user, and/or a network resource, but not to the device that is currently communicating with the computer via a specific physical communication port.

Furthermore, Richmond only teaches manipulating data packets at the network level, e.g., dropping packets or assigning priorities to received packets; however, Richmond does not teach processing based on a higher level protocol, e.g., processing based a protocol that is associated with the external device as recited by claim 10.

Regarding claim 11, Richmond does not teach a device related to an application such as synchronization applications, backup applications or other such applications. Directed to authenticating users and controlling usage of network resources, Richmond does not teach controlling a communication between a user computer and external devices such as a connected PDA or cellular phone.

Regarding claims 12, Richmond does not teach processing data that is stored in the associated buffer simply since Richmond does not teach a buffer to store a data portion. As taught by Richmond, packets are dropped or forwarded but not stored in a buffer. Likewise, elements in claims 13 and 14 related to a buffer are not taught by Richmond.

In addition, the elements of a "SCSI block" recited by claim 15, a "class driver" recited by claim 16, a "filter module" recited by claim 17, "parsing the data portion", "reassembling the data" and "analyzing the reassembled data" recited by claim 18, "security policy" recited by claim 19 and "only allowing the communication for certain working environments" recited by claim 20 are likewise not taught by Richmond.

In view of the foregoing amendments and remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Please charge any fees associated with this paper to deposit account No. 50-3355.

Respectfully submitted,

/Guy Yonay/
Guy Yonay
Attorney/Agent for Applicants
Registration No. 52,388

Dated: July 5, 2011

Pearl Cohen Zedek Latzer, LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801